

University of California



Memo
LOS ALAMOS SCIENTIFIC LABORATORY

Post Office Box 1663 Los Alamos, New Mexico 87545

In reply refer to: OS-4
Mail stop: 679

January 16, 1981

US Department of Energy
Attn: Robert O'Brien DP-35
Office of Safeguards and Security
Mail Station A2-1016
Washington, DC 20545

Dear Rob,

Enclosed in accord with your request of January 7 is our detailed comments on the draft DCID 1/16. We feel that in general the document is too complex and voluminous to be a useful policy making document. We feel it could be revised by restructuring and concentrating on the basic requirements.

Again, we offer our support to you in carrying out the DOE computer security responsibilities. I'm looking forward to meeting with you on February 9 when I will be back at DOE Headquarters.

Sincerely,

Edward A. Springer
Edward A. Springer

Attachment as stated.

EAS:njp

CYS: CRMO (2) w/o encl.
OS-4 file

COMMENTS ON DRAFT DCID 1/16

COMPUTER SECURITY SUBCOMMITTEE

General Approach

1. The document is much too long for a policy making document. It is repetitive and too detailed.
2. The document should be restructured using a different format for readability, possibly concentrating on the basic ADP security requirements with modifications for each class of systems.
3. It is not necessary to cite all the possible threats to an ADP system in this type of document. The requirements and counter-measures should be the major objective for the document.
4. The document should not be a detailed design and analysis document. It should be a general document stating the basic security requirements that the implementors can use for their design.

~~CONFIDENTIAL~~

JE

DRAFT DCID 1/16

This document is marked CONFIDENTIAL. It is intended, however, that upon review and approval, that it will be released as UNCLASSIFIED.

DRAFT

~~CONFIDENTIAL~~

DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE NO 1/16

Security of Foreign Intelligence in Automated Data
Processing Systems and Networks

Pursuant to Section 102 of the National Security Act of 1947, Executive Order 12065, and National Security Council Intelligence Directives, and in order to ensure uniform protection of classified foreign intelligence, and foreign counterintelligence involving sensitive intelligence sources and methods, processed and/or stored in Automated Data Processing (ADP) systems and networks, minimum security requirements are hereby established.

The diversity and complexity of such computer systems now in place in the Community and those already designed for future placement may not provide for compliance with the requirements of the directive in their entirety. Recognizing both the validity of the requirements and the difficulty involved in their application to currently installed and already designed ADP systems, the extent to which the exceptions to this Directive are applied to such systems is left to the determination of each National Foreign Intelligence Board (NFIB) member in view of his ultimate responsibility for the protection of intelligence information.

1. Applicability

This Directive shall apply to NFIB member agencies and all other United States Government departments and agencies which process and/or store intelligence information in ADP systems and networks. It shall apply equally when ADP systems and networks are owned and/or operated by the United States Government or by its contractors or consultants. N/C

2. Responsibilities

Each NFIB member or his designee is responsible for ensuring compliance by his respective organization and any other organization for which he has security responsibility with the provisions of this Directive and the attached Computer Security Regulation. The NFIB member or his designee may delegate this responsibility as he deems appropriate except only the NFIB member may accredit an ADP system or network for operation in the Compartmented Mode. N/C

3. Policy

A formal ADP security program shall be established and maintained to ensure that intelligence information processed and/or stored by ADP systems and networks is adequately protected. The minimum security requirements for the allowed modes of operation of ADP systems and networks are contained in the attached Computer Security Regulation. Additional ADP security measures and capabilities may be established if deemed appropriate. ADP systems involving foreign governments shall be addressed on a case-by-case basis by the NFIB members involved. N/C

4. Exceptions

a. This Directive shall not apply to the ADP systems or networks that ^{JE} are used exclusively for telecommunications services. Such systems or networks are controlled by pertinent national policies and regulations. *mk*

b. The NFIB member or his designee may temporarily exempt specific ADP systems under his jurisdiction from complete compliance with this Directive and attached Regulation when such compliance would significantly impair the execution of his mission. Chapter III of the attached Regulation governs when the ADP system being exempted is part of an ADP network as defined therein. An exemption shall be granted only when the NFIB member or his designee is confident that the other security measures in effect will adequately protect the intelligence information being processed. The NFIB member or his designee granting an exception shall strive for the earliest feasible attainment of complete compliance. No exception shall be granted which would allow personnel with less than a Secret clearance to access an ADP system or network which contains Sensitive Compartmented Information (SCI). *← URGENT
TOP SECRET*

c. Nothing in this Directive or the Computer Security Regulation shall supersede or augment the requirements on the control, use, and dissemination of Restricted Data, Formerly Restricted Data, or Communications Security (COMSEC) related material as established by or under existing statutes, directives, or Presidential policy. *mc*

Def. of SCI not included